JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11)Publication number: **08328470**
(43)Date of publication of application: **13.12.1996**

(51)Int.Cl.

G09C 1/00
G06K 17/00
H04L 9/32

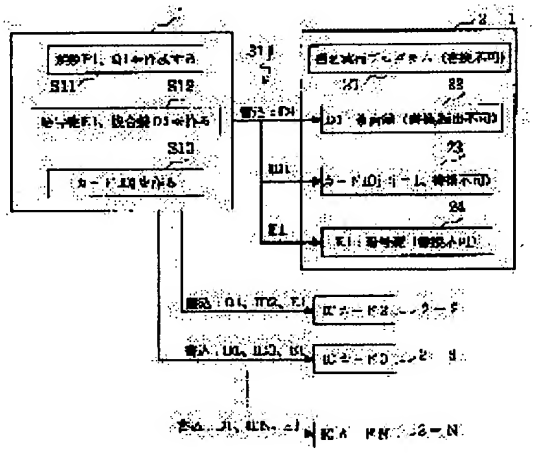
(21)Application number: **07156799**
(22)Date of filing: **31.05.1995**

(71)Applicant: **N T T DATA TSUSHIN KK**
(72)Inventor: **IEGI TOSHIATSU**

(54) KEY FORMING SYSTEM FOR DIGITAL SIGNATURE AND IC CARD FOR MAKING SIGNATURE BY USING THE KEY

(57)Abstract:

PURPOSE: To make it possible to rapidly form signature forming keys for many persons with a digital signature system.
CONSTITUTION: Just one pair of two pieces of prime numbers P1, Q1 of a large number of digits of about decimal 100 digits are formed for N persons in a key formation center 1. A pair of a cipher key E1 and a decryption key D1 are formed in accordance with therewith and N pieces of card identifiers IDj (j=1 to N) of different values are formed. The common decryption key D1 is stored as a secret key in the respective non-rewritable and non-externally readable memory areas of N sheets of IC cards 2-j (j=1 to N). The individual card identifiers IDj are otherwise stored in the non-rewritable memory areas 23. The digital signature is formed by adding the card identifiers IDj to objective information, then ciphering the set of the objective information and the card identifiers IDj with the decryption key D1 in the case the digital signature is executed by using such IC card 2-j.



LEGAL STATUS

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－328470

(43)公開日　平成８年(1996)12月13日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ　1/00		7259－5Ｊ	Ｇ０９Ｃ	1/00	
Ｇ０６Ｋ　17/00			Ｇ０６Ｋ	17/00	Ｖ
Ｈ０４Ｌ　9/32			Ｈ０４Ｌ	9/00	Ａ

審査請求　未請求　請求項の数８　ＦＤ　（全　７　頁）

(21)出願番号　特願平7－156799

(22)出願日　平成７年(1995)５月31日

(71)出願人　000102728
エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目３番３号

(72)発明者　家木　俊温
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

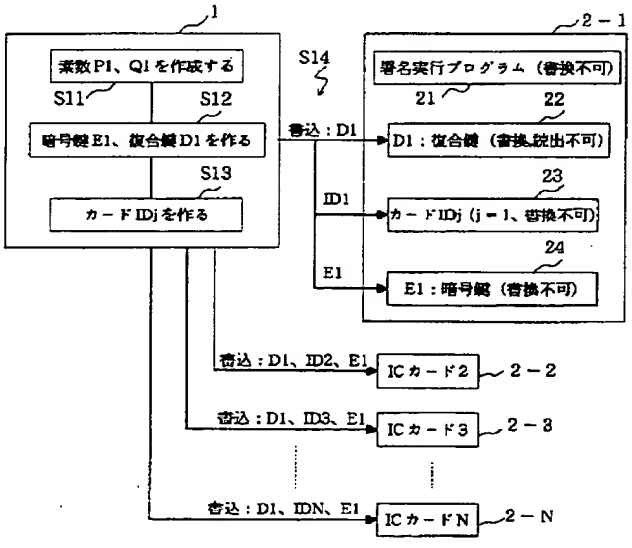
(74)代理人　弁理士　上村　輝之

(54)【発明の名称】　デジタル署名のための鍵生成方式及びその鍵を用いて署名を行うＩＣカード

(57)【要約】

【目的】　デジタル署名システムにおいて、多数の人数分の署名作成用鍵を短時間で生成できるようにする。

【構成】　鍵生成センタ１において、Ｎ人の者に対して、１０進１００桁程度の大桁数の２個の素数Ｐ１、Ｑ１を１対だけ作成し、これに基づいて１対の暗号鍵Ｅ１と復号鍵Ｄ１を生成すると共に、異なる値のＮ個のカード識別子ＩＤｊ（ｊ＝１～Ｎ）を生成する。そして、Ｎ枚のＩＣカード2－ｊ（ｊ＝１～Ｎ）の各々の、書換え不可・外部読み出し不可の記憶エリア２２に秘密鍵として共通の復号鍵Ｄ１を格納し、また、書き換え不可の記憶エリア２３に個別のカード識別子ＩＤｊを格納する。このＩＣカード2－ｊを用いてデジタル署名を行う場合、対象情報にカード識別子ＩＤｊを付加した上で、この対象情報とカード識別子ＩＤｊのセットを復号鍵Ｄ１で暗号化することによりデジタル署名を作成する。



1

【特許請求の範囲】

【請求項１】　デジタル署名のための秘密の復号鍵及び公開の暗号鍵を生成する方式において、

複数署名者に対し、共通な１対の素数に基づいて共通の１対の復号鍵及び暗号鍵を作成する共通鍵作成手段と、

前記複数署名者に対し、各人毎に異なる個別の識別子を作成する個別識別子作成手段と、

前記複数署名者に配付されるべき複数枚のＩＣカードの各々に、前記共通の復号鍵と前記個別の識別子とを書込む鍵書込み手段とを備えたことを特徴とするデジタル署名のための鍵作成方式。

【請求項２】　前記鍵書込み手段が、各ＩＣカードの書換え不可かつ外部読み出し不可の記憶エリアに前記共通の復号鍵を書込み、書換え不可の記憶エリアに前記個別の識別子を書込むことを特徴とする請求項１記載のデジタル署名のための鍵作成方式。

【請求項３】　デジタル署名のための秘密の復号鍵及び公開の暗号鍵を生成する方式において、

複数署名者に対し、桁数の比較的多い共通の１対の素数に基づいて共通の１対の復号鍵及び暗号鍵を作成する共通鍵作成手段と、

前記複数署名者に対し、桁数が比較的少なく且つ各人毎に異なる個別の複数対の素数に基づいて個別の複数対の復号鍵及び暗号鍵を作成する個別鍵作成手段と、

前記複数署名者に配付されるべき複数枚のＩＣカードの各々に、前記共通の復号鍵と前記個別の復号鍵とを書込む鍵書込み手段とを備えたことを特徴とするデジタル署名のための鍵作成方式。

【請求項４】　前記鍵書込み手段が、各ＩＣカードの書換え不可かつ外部読み出し不可の記憶エリアに前記共通の復号鍵及び前記個別の復号鍵を書込むことを特徴とする請求項１記載の鍵作成方式。

【請求項５】　デジタル署名のための秘密の復号鍵及び公開の暗号鍵を生成する方法において、

複数署名者に対し、共通な１対の素数に基づいて共通の１対の復号鍵及び暗号鍵を作成する共通鍵作成過程と、

前記複数署名者に対し、各人毎に異なる個別の識別子を作成する個別識別子作成過程と、

前記複数署名者に配付されるべき複数枚のＩＣカードの各々に、前記共通の復号鍵と前記個別の識別子とを書込む鍵書込み過程とを備えたことを特徴とするデジタル署名のための鍵作成方法。

【請求項６】　デジタル署名のための秘密の復号鍵及び公開の暗号鍵を生成する方法において、

複数署名者に対し、桁数の比較的多い共通の１対の素数に基づいて共通の１対の復号鍵及び暗号鍵を作成する共通鍵作成過程と、

前記複数署名者に対し、桁数が比較的少なく且つ各人毎に異なる個別の複数対の素数に基づいて個別の複数対の復号鍵及び暗号鍵を作成する個別鍵作成過程と、

2

前記複数署名者に配付されるべき複数枚のＩＣカードの各々に、前記共通の復号鍵と前記個別の復号鍵とを書込む鍵書込み過程とを備えたことを特徴とするデジタル署名のための鍵作成方法。

【請求項７】　記憶している秘密の復号鍵を用いてデジタル署名を作成するＩＣカードにおいて、

前記復号鍵を記憶するための書き換え不可かつ外部読出し不可の記憶エリアと、

当該ＩＣカードの識別子を記憶するための書き換え不可の記憶エリアと、

対象情報に前記識別子を付加した上で、この対象情報と識別子のセットを前記復号鍵を用いて暗号化することによりデジタル署名を作成する署名作成手段と、を備えたことを特徴とするＩＣカード。

【請求項８】　記憶している秘密の復号鍵を用いてデジタル署名を作成するＩＣカードにおいて、

第１の復号鍵及び第２の復号鍵を記憶するための書き換え不可かつ外部読出し不可の記憶エリアと、

対象情報を前記第１の復号鍵を用いて暗号化することにより第１のデジタル署名を作成して、前記対象情報に付加した上で、この対象情報と第１の復号鍵とのセットを前記第２の復号鍵を用いて暗号化することにより第２のデジタル署名を作成する署名作成手段と、を備えたことを特徴とするＩＣカード。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、例えば署名入りの金融取引証明書に用いられる署名や、ネットワークアクセス者の署名等を電子的に作成するデジタル署名に関わり、特にデジタル署名に用いる鍵の生成方式及びその鍵を用いて署名を行うためのＩＣカードに関する。

【０００２】

【従来の技術】近年、通信や金融取引等の分野においては、ある事実を証明する手段として電子的に署名を行うデジタル署名の重要性が急速に増大している。この場合、これらのシステムが大規模なことから、不特定多数の人間の誰の署名であるかを特定することが必要となる。

【０００３】ＲＳＡ（Rivest-Shamir-Adleman）暗号を署名関数として用い、秘密鍵をＩＣカードに格納する電子署名方式が知られている（特開平４－１１８７７７）。一般に、ＲＳＡ暗号を用いる署名方法では、周知のように、大きな２つの素数Ｐ、Ｑが予め選ばれ、これに基づいて規定の方法で暗号鍵と復号鍵とが作成される。

【０００４】図６は、この従来のデジタル署名作成方法を示す。鍵生成センタでは、Ｎ人の顧客に対し、２個の素数Ｐｉ、Ｑｉ（ｉ＝１～Ｎ）の対をＮ対作成し（ステップＳ１）、Ｎ対の暗号鍵Ｅｉと復号鍵Ｄｉを作成する（ステップＳ２）。そして、この暗号鍵Ｅｉと復号鍵Ｄ

ｉをそれぞれ公開鍵（＝検証鍵）、秘密鍵（＝署名鍵）としてＮ枚のＩＣカード１～Ｎにそれぞれ書き込み、各ＩＣカード１～Ｎを各顧客に渡す。各顧客は、そのＩＣカードを用いて取引文を復号鍵Ｄｉ（＝秘密鍵）で暗号化することにより、その取引文にデジタル署名を行う。署名された取引文は取引相手に送られ、そこで暗号鍵Ｅｉ（＝公開鍵）を用いて復号化されることにより、正しく署名されたものか否かが検証される。

【０００５】

【発明が解決しようとする課題】上記従来のデジタル署名作成方法では、ＲＳＡ暗号で必要な強度を保つため、素数Ｐｉ、Ｑｉとして、１０進１００桁程度の極めて大きい数を用いる必要がある。そのため、１対の暗号鍵Ｅｉ及び復号鍵Ｄｉを作成するために、一般に数分程度の時間がかかる。従って、多数の人数分の鍵を作成する場合には膨大な時間を必要とし、実現性に乏しいという問題点がある。

【０００６】本発明は上記従来の問題点に鑑み、多数の人数分の鍵を短時間で作成することができるデジタル署名用鍵の生成方式を提供することを目的とする。

【０００７】また、本発明の別の目的は、そのように作成された鍵を用いて安全性の高いデジタル署名を作成することのできるＩＣカードを提供することにある。

【０００８】

【課題を解決するための手段】本発明の第１の側面に従うデジタル署名用鍵の生成方式は、複数人の署名者に対し、共通な１対の素数に基づいて共通の１対の復号鍵及び暗号鍵を作成する共通鍵作成手段と、上記複数署名者に対し、各人毎に異なる個別の識別子を作成する個別識別子作成手段と、上記複数署名者に配付されるべき複数枚のＩＣカードの各々に、上記共通の復号鍵と上記個別の識別子とを書込む鍵書込み手段とを備えたことを特徴とする。

【０００９】この方式において、望ましくは、ＩＣカードの書換え不可かつ外部読み出し不可の記憶エリアに上記共通の復号鍵が書込まれ、書換え不可の記憶エリアに上記個別の識別子が書込まれる。

【００１０】本発明の第２の側面に従う鍵生成方式は、複数署名者に対し、桁数の比較的多い共通の１対の素数に基づいて共通の１対の復号鍵及び暗号鍵を作成する共通鍵作成手段と、上記複数署名者に対し、桁数が比較的少なく且つ各人毎に異なる個別の複数対の素数に基づいて個別の複数対の復号鍵及び暗号鍵を作成する個別鍵作成手段と、上記複数署名者に配付されるべき複数枚のＩＣカードの各々に、上記共通の復号鍵と個別の復号鍵とを書込む鍵書込み手段とを備えたことを特徴とする。

【００１１】この方式では、望ましくは、ＩＣカードの書換え不可かつ外部読み出し不可の記憶エリアに上記共通の復号鍵及び個別の復号鍵が書込まれる。

【００１２】本発明の第３の側面に従うデジタル署名用

のＩＣカードは、秘密鍵たる復号鍵を記憶するための書き換え不可かつ外部読出し不可の記憶エリアと、当該ＩＣカードの識別子を記憶するための書き換え不可の記憶エリアと、対象情報に上記識別子を付加した上で、この対象情報と識別子のセットを上記復号鍵を用いて暗号化することによりデジタル署名を作成する署名作成手段とを備えたことを特徴とする。

【００１３】本発明の第４の側面に従うデジタル署名用のＩＣカードは、秘密鍵たる第１の復号鍵及び第２の復号鍵を記憶するための書き換え不可かつ外部読出し不可の記憶エリアと、対象情報を第１の復号鍵を用いて暗号化することにより第１のデジタル署名を作成して、これを対象情報に付加した上で、この対象情報と第１の復号鍵とのセットを第２の復号鍵を用いて暗号化することにより第２のデジタル署名を作成する署名作成手段とを備えたことを特徴とする。

【００１４】

【作用】本発明の第１又は第２の側面に従う鍵生成方式では、複数人の署名者に対し、共通の１対の素数に基づいて共通の暗号鍵及び復号鍵を作成し、また、各人毎に異なる個別の識別子又は個別の暗号鍵及び復号鍵を作成し、この共通の復号鍵（秘密鍵）と個別の識別子又は個別の復号鍵（秘密鍵）とを各人のＩＣカードに書込む。この作成方式によれば、複数人に対して共通の暗号鍵及び復号鍵を作るため、大きな桁数の素数からこの共通鍵を作成する場合でも、各人毎にそれを行う必要がないため、多数の人数分の鍵を短時間で作成することができる。しかも、この共通の鍵は、個別の識別子又は個別の鍵と共にＩＣカードに書込まれるので、ＩＣカードで署名を作成する際には、共通の鍵と個別の識別子又は個別の鍵とを組合せて用いることにより、各人にユニークな署名を作成でき、よって、署名としての機能が十分に果たせる。尚、個別の識別子や個別の鍵の作成作業については、識別子のそれは単に異なるコードを決めるだけであり、個別の鍵のそれは桁数の少ない素数から作るものであるため、いずれも短時間で行える。

【００１５】ＩＣカード内では、秘密鍵としての復号鍵は、ＩＣカードの書換え不可かつ外部読み出し不可の記憶エリアに記憶されることが望ましい。それにより、署名を他者が偽造するこが不可能となりセキィリティが確保される。

【００１６】本発明の第３又は第４の側面に従うＩＣカードでは、記憶している秘密鍵たる復号鍵と識別子の双方を用いて、又は記憶している複数個の復号鍵を用いて対象情報を暗号化して署名を作成する。そのため、記憶している復号鍵と識別子とのセット、又は複数個の復号鍵のセットがそのＩＣカードにユニークでありさえすれば、記憶している復号鍵の内の少なくとも１つが他のＩＣカードと共通であっても、当該ＩＣカードにユニークな署名を作成することが可能である。その結果、複数署

名者に共通の鍵を用いることが可能となるので、ＩＣカード発行元において鍵を予め作成する処理時間が短縮され、多数人に対してＩＣカード発行することが容易になる。

【００１７】

【実施例】以下、図面を参照して本発明の実施例を説明する。図１は本発明を適用したデジタル署名システムの一実施例の全体構成を示す。

【００１８】図１において、鍵生成センタ１は、ＲＳＡ暗号を用いて多数の顧客に対する鍵を生成し、それぞれの顧客の鍵をそれぞれの顧客用のＩＣカードに書込む作業を行うものである。この鍵生成センタ１は、まず、所定人数（＝Ｎ人）の顧客のグループに対して、１０進１００桁程度の大きい２個の素数Ｐ１、Ｑ１を１対だけ作成し（ステップＳ１１）、この素数Ｐ１、Ｑ１に基づいて１対の暗号鍵Ｅ１と復号鍵Ｄ１を作成する（ステップＳ１２）。次いで、鍵生成センタ１は、互いに異なる値をもつＮ個のカード識別子ＩＤｊ（ｊ＝１～Ｎ）を作成する（ステップＳ１３）。

【００１９】こうして１対の暗号鍵Ｅ１と復号鍵Ｄ１と、Ｎ個のカード識別子ＩＤｊ（ｊ＝１～Ｎ）とを用意すると、次に、鍵生成センタ１は、暗号鍵Ｅ１と復号鍵Ｄ１とカード固有のカード識別子ＩＤｊとを予め用意したＮ枚のＩＣカード２-ｊ（ｊ＝１～Ｎ）に書込む（ステップＳ１４）。

【００２０】ここで、一般にＩＣカードは周知のように、プログラムされたＣＰＵとデータ等を格納する半導体メモリとを内蔵したＩＣチップを有しており、半導体メモリ内の任意の記憶エリアに対し書き換え不可、読み出し不可（＝ＩＣチップ外への読出し不可）等の種々のアクセス規制を施すようプログラムされることができる。鍵生成センタ１に用意された各ＩＣカード２-ｊは、署名実行プログラムがその書換え不可エリア２１に予め格納されている。そして、鍵生成センタ１は、上記復号鍵Ｄ１を秘密鍵として各ＩＣカード２-ｊの書換え不可及び読み出し不可のエリア２２に、そのカード固有のカード識別子ＩＤｊを書換え不可エリア２３に、また、上記暗号鍵Ｅ１を公開鍵として書換え不可エリア２４に書き込む。

【００２１】このようにして、鍵生成センタ１は、所定のＮ人の顧客に対して、共通の暗号鍵Ｅ１と復号鍵Ｄ１と個別のカード識別子ＩＤｊとを書込んだＩＣカードＩＣカード２-ｊ（ｊ＝１～Ｎ）を発行する。その後、鍵生成センタ１は、次のＮ人の顧客のグループに対し、前のグループとは異なる新たな２個の素数Ｐ２、Ｑ２を１対作成し、これに基づき１対の暗号鍵Ｅ２と復号鍵Ｄ２を作成し、また、前のグループと同じＮ個のカード識別子ＩＤｊ（ｊ＝１～Ｎ）を作成し、これらを新たなＮ枚のＩＣカード２-ｊ（ｊ＝Ｎ＋１～２Ｎ）に書込んで発行する。以下、同様の処理を繰り返す。

【００２２】以上のように、鍵生成センタ１は所定の複数人（Ｎ人）に対して１対の暗号鍵Ｅ１と復号鍵Ｄ１を割り当てるので、多数の人数分の鍵を短時間で作成することができる。また、発行されたＩＣカード２-ｊでは、秘密鍵（＝署名鍵）としての復号鍵Ｄ１が書換え不可及び読み出し不可のエリアに格納されているため、鍵生成センタ１以外の者がそのＩＣカードを偽造することはできない。

【００２３】図２は、本実施例において顧客がＩＣカードを用いてデジタル署名を行う場合の処理流れを示す。

【００２４】顧客が商品購入等の取引を行った際、顧客所持のＩＣカード２-ｎが所定のカード用端末装置（図示せず）にセットされる。すると、ＩＣカード２-ｎは、図２に示すように署名実行プログラムに従って、まず、端末から取引内容を記述した対象情報３０を取り込み（ステップＳ１５）、この対象情報３０にカード識別子ＩＤｎを付加し（ステップＳ１６）、この対象情報３０とカード識別子ＩＤｎのセットを復号鍵Ｄ１で暗号化することによりデジタル署名３１を作成して、この署名３１を上記セットに付加する（ステップＳ１７）。こうして作成された対象情報３０とカード識別子ＩＤｎとデジタル署名３１のセットは、ＩＣカード２-ｎから端末を通じて取引相手へ電子的に送信される。

【００２５】図３は一例として電話ショッピングの場合のデジタル署名の処理形態を示す。

【００２６】顧客４０が通信回線４１を介して商品販売者４２に対して商品を注文し（ステップＳ２１）、商品販売者４２が購入内容を示す情報４３を顧客４０に送信する（ステップＳ２２）。顧客４０はその購入内容情報４３を確認した後、自己のＩＣカード２-ｎを用いてその購入内容情報４３に自己のカード識別子ＩＤｎを付加し、購入内容情報４３とカード識別子ＩＤｎのセットを秘密鍵たる復号鍵Ｄ１で暗号化することによりデジタル署名４４を作成し、 このデジタル署名４４を購入内容情報４３と識別子ＩＤｎとのセットに付加し（ステップＳ２３）、そして、この署名を付加した情報を商品販売者４２に返信する（ステップＳ２４）。商品販売者４２は、返信された情報を購入内容情報４３、識別子ＩＤｎ及び署名４４に分離した上で、署名４４を公開鍵たる暗号鍵Ｅ１で復号化することにより元の購入内容情報４３と識別子ＩＤｎを復元し、この復元した購入内容情報４３と識別子ＩＤｎとを返信されたそれと照合することにより、正しい署名か否かを検証する。正しい署名であることが確認できると、商品販売者４２は購入内容情報４３を保管し、そして商品を顧客に配送する（ステップＳ２５）。

【００２７】以上のように、Ｎ人の顧客に秘密鍵（＝署名鍵）として共通の復号鍵Ｄ１を付与していても、複合鍵Ｄ１とカード識別子ＩＤｎとのセットは各顧客にユニークであるために、カード識別子ＩＤｎと復号鍵Ｄ１と

を用いてデジタル署名を行うことにより、デジタル署名は各顧客にユニークなものとなり署名としての機能を果たすことができる。しかも、秘密鍵（＝署名鍵）たる復号鍵Ｄ１は、書き換えもＩＣチップ外への読出しも不可能であるため、署名の偽造は不可能であり署名の信頼性が確保される。

【００２８】次に、図４及び図５を参照して本発明の第２の実施例を説明する。図４は第２の実施例の全体の構成を示し、図５はＩＣカードによりデジタル署名を行う場合の処理流れを示す。

【００２９】図４に示すように、鍵生成センタ５０は、まず、前実施例と同様に所定のＮ人の顧客のグループに対し、１０進１００桁程度の大桁数の２個の素数Ｐ１、Ｑ１を１対作成し（ステップＳ３１）、これに基づき１対の暗号鍵Ｅ１と復号鍵Ｄ１を作成し（ステップＳ３２）、次いで、Ｎ個のカード識別子ＩＤｊ（ｊ＝１～Ｎ）を作成する（ステップＳ３３）。次に、上記素数Ｐ１、Ｑ１より桁数が少ない２個の素数ｐｊ、ｑｊをＮ対作成し（ステップＳ３４）、それらに基づきＮ対の暗号鍵ｅｊと復号鍵ｄｊを作成する（ステップＳ３５）。そして、Ｎ枚のＩＣカード５１-ｊ（ｊ＝１～Ｎ）に、上記共通の暗号鍵Ｅ１及び復号鍵Ｄ１と、上記個別のカード識別子ＩＤｊ、暗号鍵ｅｊ及び復号鍵ｄｊとをそれぞれ書込んで（ステップＳ３６）、上記Ｎ人の顧客にそれぞれ発行する。

【００３０】この後、鍵生成センタ５０は、次のＮ人の顧客のグループに対し、別の新たな大桁数の素数Ｐ２、Ｑ２を作成して１対の暗号鍵Ｅ２と復号鍵Ｄ２を作成し、この暗号鍵Ｅ２及び復号鍵Ｄ２と、前の顧客グループと同じ個別のカード識別子ＩＤｊ、暗号鍵ｅｊ及び復号鍵ｄｊとを、次のＮ枚のＩＣカード５１-ｊ（ｊ＝Ｎ＋１～２Ｎ）に書込んで発行する。以下、同様の処理を繰り返す。

【００３１】この実施例では、Ｎ対の暗号鍵ｅｊ及び復号鍵ｄｊを生成するが、その素となる素数ｐｊ、ｑｊの桁数が少ないので、比較的短時間で生成することができる。

【００３２】各ＩＣカード５１-ｊでは、署名実行プログラムが書換え不可エリア５２に、共通の復号鍵Ｄ１が秘密鍵（＝署名鍵）として書換え不可・読み出し不可エリア５３に、個別のカード識別子ＩＤｊが書換え不可エリア５４に、共通の暗号鍵Ｅ１が公開鍵（＝検証鍵）として書換え不可エリア５５に、個別の復号鍵ｄｊが秘密鍵（＝署名鍵）として書き換え不可・読み出し不可エリア５６に、個別の暗号鍵ｅｊが公開鍵（＝検証鍵）として書換え不可エリア４７にそれぞれ格納される。

【００３３】顧客が自己のＩＣカード５１-ｎを用いてデジタル署名を行う場合には、図５に示すように署名実行プログラムに従い、まず対象情報６０を端末から取り込み（ステップＳ３７）、この対象情報６０を共通の復号鍵Ｄ１で暗号化して第１の署名６１を作成して、この第１の署名６１を対象情報６０に付加し（ステップＳ３８）、更に、対象情報６０と署名６１のセットを個別の復号鍵ｄｊで暗号化して第２の署名６２を作成して、この第２の署名６２を更に付加する（ステップＳ３９）。こうして作成された対象情報６０と署名６１と第２の署名６２のセットが、ＩＣカード５１-ｎから端末を通じて取引相手に送信される。

【００３４】この第２の実施例によれば、複数人に対し、比較的大きな桁数の素数Ｐ１、Ｑ１に基づいて共通の１対の暗号鍵Ｅ１と復号鍵Ｄ１を作成し、かつ比較的小さな桁数の素数ｐｊ、ｑｊに基づいて個別の暗号鍵ｅｊと復号鍵ｄｊを作成して割り当てるので、従来例のように大きな桁数の素数Ｐｊ、Ｑｊに基づいて個別の暗号鍵Ｅｊと復号鍵Ｄｉを作成する場合に比較し短時間で鍵を作成できると共に、個別の鍵を用いない前の実施例より一層高いセキュリティを確保することができる。

【００３５】

【発明の効果】以上説明したように本発明によれば、多数の人数分の鍵を短時間で作成することができるので、多数人を対象とするデジタル署名システムの実現に貢献できる。

【図面の簡単な説明】

【図１】本発明を適用したデジタル署名システムの一実施例の構成を示すブロック図である。

【図２】同実施例においてＩＣカードによりデジタル署名を行う場合の処理流れを示すフローチャートである。

【図３】同実施例を用いて電話ショッピングで署名を行う場合の処理流れを示すフローチャートである。

【図４】本発明の第２の実施例の構成を示すブロック図である。

【図５】この第２実施例においてＩＣカードによりデジタル署名を行う場合の処理流れを示すフローチャートである。

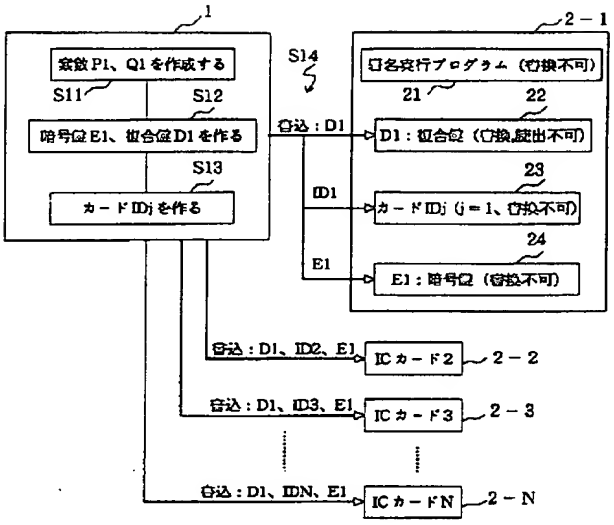
【図６】従来のデジタル署名方式を示すブロック図である。

【符号の説明】

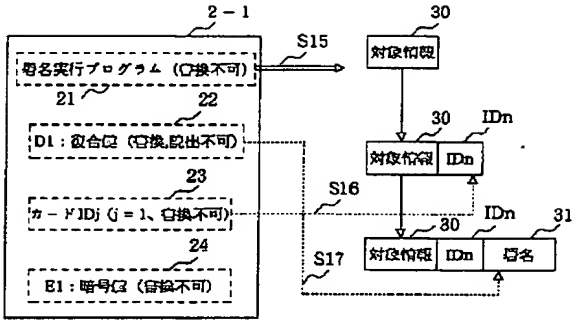
１、５０　鍵生成センタ

２、５１　ＩＣカード

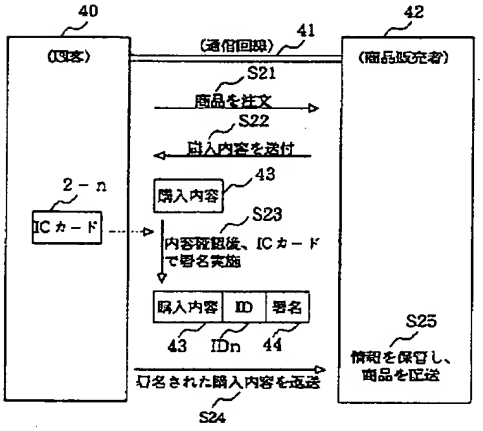
【図１】


1
2－1
素数P1、Q1を作成する
S11
S12
暗号鍵E1、復合鍵D1を作る
S13
カードIDjを作る
S14
署名実行プログラム（改竄不可）
21
22
書込：D1
D1：復合鍵（改竄,読出不可）
23
ID1
カードIDj（j＝1、改竄不可）
24
E1
E1：暗号鍵（改竄不可）
書込：D1、ID2、E1
ICカード2
2－2
書込：D1、ID3、E1
ICカード3
2－3
書込：D1、IDN、E1
ICカードN
2－N

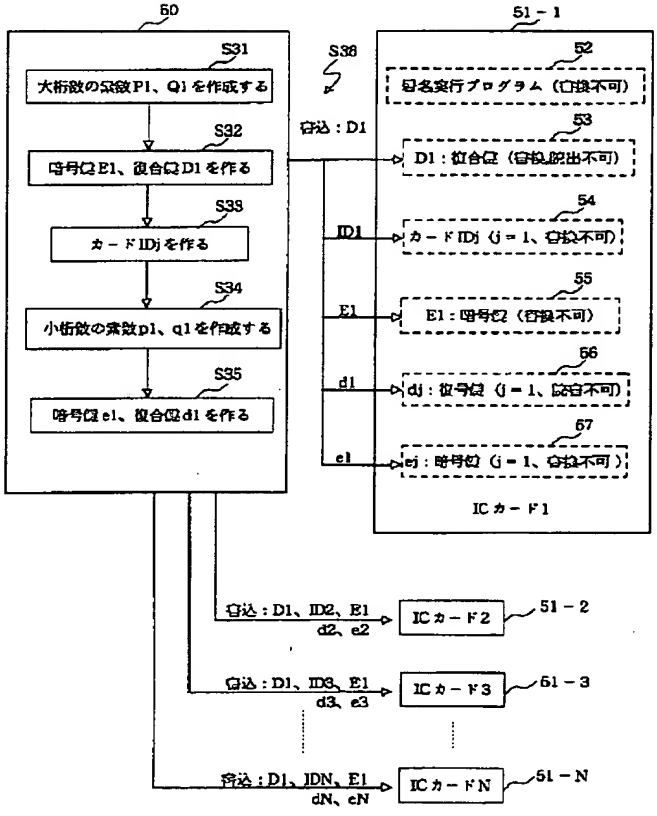
【図２】


2－1
署名実行プログラム（改竄不可）
21
22
D1：復合鍵（改竄,読出不可）
23
カードIDj（j＝1、改竄不可）
24
E1：暗号鍵（改竄不可）
S15
30
対応情報
IDn
S16
S17
31
署名

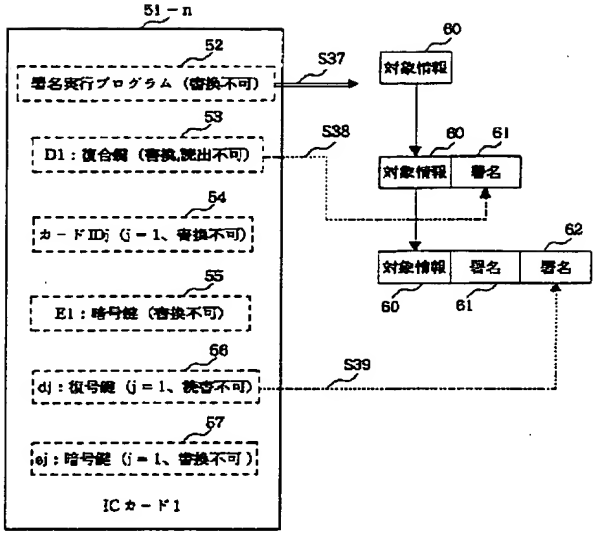
【図３】


40
(顧客)
41
(通信回線)
42
(商品販売者)
S21
商品を注文
S22
購入内容を送付
2－n
ICカード
購入内容
43
S23
内容確認後、ICカードで署名実施
購入内容
ID
署名
43
IDn
44
S25
情報を保管し、商品を配送
署名された購入内容を送信
S24

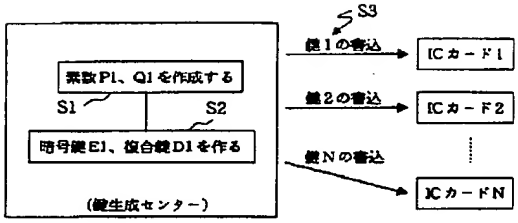
【図４】


50
51－1
S31
大桁数の素数P1、Q1を作成する
S32
暗号鍵E1、復合鍵D1を作る
S33
カードIDjを作る
S34
小桁数の素数p1、q1を作成する
S35
暗号鍵e1、復合鍵d1を作る
S36
書込：D1
52
署名実行プログラム（改竄不可）
53
D1：復合鍵（改竄,読出不可）
ID1
54
カードIDj（j＝1、改竄不可）
E1
55
E1：暗号鍵（改竄不可）
d1
56
dj：復号鍵（j＝1、読出不可）
e1
57
ej：暗号鍵（j＝1、改竄不可）
ICカード1
書込：D1、ID2、E1
d2、e2
ICカード2
51－2
書込：D1、ID3、E1
d3、e3
ICカード3
51－3
書込：D1、IDN、E1
dN、eN
ICカードN
51－N

【図５】


51－n
52
署名実行プログラム（書換不可）
53
D1：復合鍵（書換,読出不可）
54
カードIDj（j＝1、書換不可）
55
E1：暗号鍵（書換不可）
56
dj：復号鍵（j＝1、読出不可）
57
ej：暗号鍵（j＝1、書換不可）
ICカード1
S37
S38
S39
60
対象情報
61
署名
62

【図６】


素数P1、Q1を作成する
S1
S2
暗号鍵E1、復合鍵D1を作る
（鍵生成センター）
S3
鍵1の書込
鍵2の書込
鍵Nの書込
ICカード1
ICカード2
ICカードN